

- 1 1. A method for dial roaming for users having a home non-LDAP
2 (Lightweight Directory Access Protocol) region to allow access comprising:
3 dialing into a local dial access provider;
4 creating an access request ;
5 forwarding the dial access request to a corporate remote authentication dial-in
6 user service (RADIUS) server;
7 proxying the request to a regional RADIUS server associated with the user's
8 home region;
9 accessing the regional user database to determine if the user is present in the
10 regional database;
11 authenticating the user; and
12 providing configuration information to the user to allow access to the network.
13 2. The method for dial roaming of claim 1 wherein the access request is
14 forwarded to an access provider via a network access server (NAS).
15 3. The method of claim 2 wherein the NAS functions as a client of the
16 corporate RADIUS server.
17 4. The method of claim 1 further comprising:
18 the corporate RADIUS server determining if the user is a member of an LDAP or
19 non-LDAP region.
20 5. The method of claim 4 wherein the determining if the user is a member of an
21 LDAP or non-LDAP region is accomplished by reviewing a configuration file
22 stored in the corporate RADIUS server.

- 1 6. The method of claim 1 further comprising forwarding the access request to a
- 2 regional LDAP database if the home region is LDAP enabled.
- 3 7. The method of claim 6 further comprising the regional LDAP database
- 4 authenticating the user.
- 5 8. The method of claim 7 further comprising the regional LDAP database
- 6 sending an “accept” message if the user is in the regional LDAP database and a
- 7 “deny” message if the user is not in the regional LDAP database.
- 8 9. The method of claim 1 wherein the access request comprises a user name and
- 9 password.
- 10 10. The method of claim 9 wherein the user name comprises a regional naming
- 11 convention for identifying the home region of the user.
- 12 11. The method of claim 9 wherein the user name comprises an email address of
- 13 the user.
- 14 12. the method of claim 9 further comprising comparing the user password to the
- 15 password stored in the non-LDAP database.
- 16 13. The method of claim 12 wherein the password from the database is CHAP
- 17 hashed, and wherein the password delivered to the database is CHAP hashed, and
- 18 wherein the password comparison comprises comparing the CHAP hashed
- 19 password delivered to the database with the CHAP hashed password extracted
- 20 from the database.
- 21 14. The method of claim 12 wherein the database of the non-LDAP regions is an
- 22 subscriber management system (SMS) database.
- 23 15. The method of claim 9 wherein the password is hashed to maintain security.

16. A system for dial roaming for users having a home non-LDAP region to allow access comprising:

a user computer having a home service region for creating a network access request;

a dial up connection over a first network to a network access server (NAS) in a roaming area:

a second network connected to the NAS for receiving the network access request;

a local network service provider connected to the second network;

a third network connected to the network service provider;

a corporate RADIUS server connected to the third network for receiving the access request; and

a regional LDAP server comprising a user database for authenticating the user access request and for allowing access to the regional network.

17. The system of claim 16 further comprising a regional RADIUS server connected to a non-LDAP regional server connected to the second network for receiving the access request.

18. The system of claim 17 wherein the non-LDAP regional server further comprises a user database and access instructions for authenticating the user access request in the non-LDAP server database.

19. The system of claim 18 wherein the database is an SMS database.

20. The system of claim 16 wherein the user access request comprises a user ID and password.

1 26. The system for authenticating users using a standard RADIUS protocol
 2 against a non-standard subscriber management system and database of claim 24
 3 wherein the
 4 password from the user database is CHAP hashed to compare to the password
 5 presented in the user access request.

6 27. The system for authenticating users using a standard RADIUS protocol
 7 against a non-standard subscriber management system and database of claim 26
 8 wherein the subscriber management server further comprises instructions for
 9 sending an "accept" message to the RADIUS server if the user password from the
 10 user database matches the user password presented in the user access request, and
 11 for sending a "deny" message to the RADIUS server if the user password from
 12 the user database does not matche the user password presented in the user access
 13 request.

14
 15
 16
 17